

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-047987

(43)Date of publication of application : 18.02.2000

(51)Int.Cl.

G06F 15/00
H04L 9/32
// G06F 17/30

(21)Application number : 10-214983

(71)Applicant : FUJI PHOTO FILM CO LTD

(22)Date of filing : 30.07.1998

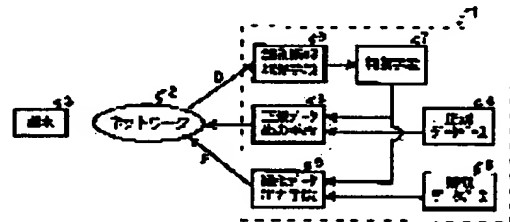
(72)Inventor : NAKAMURA ATSUSHI
ITO WATARU

(54) METHOD AND DEVICE FOR OUTPUTTING DATA, AND STORAGE MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To prevent data from flowing to a person illegally accessing a data base or the like.

SOLUTION: A judging means 7 judges whether identification information D acquired from a terminal 3 is regular or not. When it is regular, regular data T are read out of a regular data base 4 and the regular data T are outputted from a regular data output means 8 to the terminal 3. When the identification information D is not regular, dummy data F similar to the regular data T but different from them are read out of a dummy data base 5 and the dummy data F are outputted from a dummy data output means 9 to the terminal 3. Thus, even in the case of illegal access, since any data are acquired at the terminal 3, the illegally accessing person has the illusion of making the access successful.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2000-47987
(P2000-47987A)

(43) 公開日 平成12年2月18日 (2000.2.18)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード [*] (参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 A 5 B 0 7 5
H 0 4 L 9/32		H 0 4 L 9/00	6 7 1 5 B 0 8 5
// G 0 6 F 17/30		G 0 6 F 15/40	3 2 0 Z 5 K 0 1 3

審査請求 未請求 請求項の数15 O L (全 7 頁)

(21) 出願番号 特願平10-214983

(22) 出願日 平成10年7月30日 (1998.7.30)

(71) 出願人 000005201

富士写真フイルム株式会社
神奈川県南足柄市中沼210番地

(72) 発明者 中村 淳

神奈川県足柄上郡開成町宮台798番地 富
士写真フイルム株式会社内

(72) 発明者 伊藤 渡

神奈川県足柄上郡開成町宮台798番地 富
士写真フイルム株式会社内

(74) 代理人 100073184

弁理士 柳田 征史 (外1名)

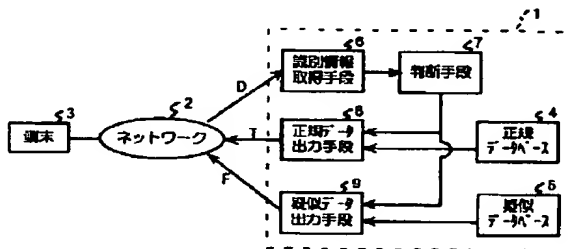
Fターム(参考) 5B075 KK43 KK54 KK63 ND02 PQ12
5B085 AC03 AE01 AE06
5K013 GA02

(54) 【発明の名称】 データ出力方法および装置並びに記録媒体

(57) 【要約】

【課題】 データベース等への不正アクセス者に対するデータの流出を防止する。

【解決手段】 端末3から取得した識別情報Dが正規のものであるか否かを判断手段7において判断する。正規のものである場合には、正規データベース4から正規データTを読み出し、正規データ出力手段8より正規データTを端末3に出力する。識別情報Dが正規のものでない場合には、正規データTとは似て非なる疑似データFを疑似データベース5から読み出し、疑似データ出力手段9より疑似データFを端末3に出力する。これにより、不正アクセスの場合でも、何らかのデータが端末3において取得されるため、不正アクセス者に対してアクセスに成功したかのような錯覚を起こさせることができる。



【特許請求の範囲】

【請求項1】 データを取得するための識別情報の取得に基づいて、前記識別情報に対応する正規データの出力を許容するか否かを判断し、前記正規データを出力することが許容された場合に、該正規データを出力するデータ出力方法において、

前記正規データを出力することが許容されなかった場合に、前記正規データとは異なる疑似データを出力することを特徴とするデータ出力方法。

【請求項2】 前記疑似データを、該疑似データを蓄積する疑似データ蓄積手段から出力することを特徴とする請求項1記載のデータ出力方法。

【請求項3】 前記疑似データを前記正規データに基づいて作成することを特徴とする請求項1記載のデータ出力方法。

【請求項4】 前記正規データが数値を配列した数値データの場合、前記疑似データは前記正規データの数値をランダムに配置した数値データであることを特徴とする請求項1から3のいずれか1項記載のデータ出力方法。

【請求項5】 前記取得された識別情報を所定形式の比較識別情報と比較し、前記取得した識別情報が前記比較識別情報と異なる場合には、前記正規データおよび前記疑似データの出力を禁止することを特徴とする請求項1から4のいずれか1項記載のデータ出力方法。

【請求項6】 正規データを蓄積した正規データ蓄積手段と、

前記正規データを取得するための識別情報を取得する識別情報取得手段と、

該識別情報取得手段により取得された前記識別情報に基づいて、該識別情報に対応する正規データの出力を許容するか否かを判断する判断手段と、

該判断手段により前記正規データを出力することが許容された場合に、該正規データを出力する正規データ出力手段とを備えたデータ出力装置において、

前記判断手段により前記正規データを出力することが許容されなかった場合に、前記正規データとは異なる疑似データを出力する疑似データ出力手段をさらに備えたことを特徴とするデータ出力装置。

【請求項7】 前記疑似データを蓄積する疑似データ蓄積手段をさらに備えたことを特徴とする請求項6記載のデータ出力装置。

【請求項8】 前記正規データに基づいて前記疑似データを作成する疑似データ作成手段をさらに備えたことを特徴とする請求項6記載のデータ出力装置。

【請求項9】 前記正規データが数値を配列した数値データの場合、前記疑似データは前記正規データの数値をランダムに配置した数値データであることを特徴とする請求項6から8のいずれか1項記載のデータ出力装置。

【請求項10】 前記入力された識別情報を所定形式の

比較識別情報と比較する比較手段と、

前記取得した識別情報が前記比較識別情報と異なる場合には、前記正規データおよび前記疑似データの出力を禁止する禁止手段とをさらに備えたことを特徴とする請求項6から9のいずれか1項記載のデータ出力装置。

【請求項11】 データを取得するための識別情報の取得に基づいて、前記識別情報に対応する正規データの出力を許容するか否かを判断し、前記正規データを出力することが許容された場合に、該正規データを出力するデータ出力方法をコンピュータに実行させるためのプログラムを記録したコンピュータ読取り可能な記録媒体において、

前記プログラムは、前記正規データを出力することが許容されなかった場合に、前記正規データとは異なる疑似データを出力する手順を有することを特徴とするコンピュータ読取り可能な記録媒体。

【請求項12】 前記疑似データを出力する手順は、前記疑似データを、該疑似データを蓄積する疑似データ蓄積手段から出力する手順であることを特徴とする請求項11記載のコンピュータ読取り可能な記録媒体。

【請求項13】 前記疑似データを前記正規データに基づいて作成する手順をさらに有することを特徴とする請求項11記載のコンピュータ読取り可能な記録媒体。

【請求項14】 前記正規データが数値を配列した数値データの場合、前記疑似データは前記正規データの数値をランダムに配置した数値データであることを特徴とする請求項11から13のいずれか1項記載のコンピュータ読取り可能な記録媒体。

【請求項15】 前記取得された識別情報を所定形式の比較識別情報と比較する手順と、

前記取得した識別情報が前記比較識別情報と異なる場合には、前記正規データおよび前記疑似データの出力を禁止する手順とをさらに有することを特徴とする請求項11から14のいずれか1項記載のコンピュータ読取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ID等の識別情報を取得し、この識別情報に基づいてデータを出力するデータ出力方法および装置並びにデータ出力方法をコンピュータに実行させるためのプログラムを記録したコンピュータ読取り可能な記録媒体に関するものである。

【0002】

【従来の技術】近年、ネットワークを介して種々のデータのやり取りが行われている。このようにネットワークを介してやり取りされるデータには、機密性の高いもの、個人的なデータ、著作権により保護されるべきデータ等が含まれている。したがって、これらのデータを暗号化したり、キーワードを用いたりする等して、特定の者以外の不正アクセス者によるデータへのアクセスを禁

止することにより、これらのデータを不正な利用から保護する必要がある。このようなデータ保護の方式としては、例えば、電子化された画像データに暗号化情報を埋め込む方式（特開平5-236424号）、媒体に固有番号を付与し、この媒体固有番号に対してのみソフトウェアの実行を許可する方式（特開平5-257816号）、共通鍵を用いる方式において、共通鍵により暗号化された情報本体と利用条件情報とを別の記憶部に記憶しておき、情報の改竄を検出する方式（特開平7-131452号）等が知られている。これらの方式は、暗号、キーワード、固有番号等が一致しない場合には、データの表示や提供を禁止するものであり、不正なアクセスを行った者に対してアクセスが失敗したことを告知するものである。

【0003】

【発明が解決しようとする課題】しかしながら、これらの方式においては、暗号やキーワードを何回も入力し直すことにより、いずれは暗号やキーワードが解読されるおそれがあり、その結果データが不正アクセス者に流出するおそれがある。

【0004】本発明は上記事情に鑑みなされたものであり、不正アクセス者に対するデータの流出を防止できるデータ出力方法および装置並びにデータ出力方法をコンピュータに実行させるためのプログラムを記録したコンピュータ読取り可能な記録媒体を提供することを目的とするものである。

【0005】

【課題を解決するための手段】本発明によるデータ出力方法は、データを取得するための識別情報の取得に基づいて、前記識別情報に対応する正規データの出力を許可するか否かを判断し、前記正規データを出力することが許可された場合に、該正規データを出力するデータ出力方法において、前記正規データを出力することが許可されなかった場合に、前記正規データとは異なる疑似データを出力することを特徴とするものである。

【0006】ここで、「疑似データ」とは、正規データと似て非なるデータのように、不正アクセス者がアクセスに失敗したことを自覚しない程度のデータのことをいい、例えば画像データの場合は正規データのように見えるが正規データにより表される画像と類似した色調あるいは類似した構図の画像を表す画像データ、数値を配列したデータの場合はその数値の並び方、数値の内容、桁数、データ形式等を変更したデータのことをいう。

【0007】また、「識別情報を取得する」とは、アクセス者が自ら識別情報を入力する場合の他、アクセスされた端末の端末IDを自動的に取得する、あるいは電話回線を使用してアクセスされた場合には端末の電話番号を自動的に取得する場合を含むものである。

【0008】なお、前記疑似データを、該疑似データを蓄積する疑似データ蓄積手段から出力するようにしても

よく、前記疑似データを前記正規データに基づいて作成するようにしてもよい。

【0009】また、前記正規データが数値を配列した数値データの場合、前記疑似データは前記正規データの数値をランダムに配置した数値データとすることが好ましい。

【0010】さらに、前記取得された識別情報を所定形式の比較識別情報と比較し、前記取得した識別情報が前記比較識別情報と異なる場合には、前記正規データおよび前記疑似データの出力を禁止することが好ましい。

【0011】本発明によるデータ出力装置は、正規データを蓄積した正規データ蓄積手段と、前記正規データを取得するための識別情報を取得する識別情報取得手段と、該識別情報取得手段により取得された前記識別情報に基づいて、該識別情報に対応する正規データの出力を許可するか否かを判断する判断手段と、該判断手段により前記正規データを出力することが許可された場合に、該正規データを出力する正規データ出力手段とを備えたデータ出力装置において、前記判断手段により前記正規データを出力することが許可されなかった場合に、前記正規データとは異なる疑似データを出力する疑似データ出力手段をさらに備えたことを特徴とするものである。

【0012】なお、前記疑似データを蓄積する疑似データ蓄積手段をさらに備えるようにしてもよく、前記正規データに基づいて前記疑似データを作成する疑似データ作成手段をさらに備えるようにしてもよい。

【0013】また、前記正規データが数値を配列した数値データの場合、前記疑似データは前記正規データの数値をランダムに配置した数値データであることが好ましい。

【0014】さらに、前記入力された識別情報を所定形式の比較識別情報と比較する比較手段と、前記取得した識別情報が前記比較識別情報と異なる場合には、前記正規データおよび前記疑似データの出力を禁止する禁止手段とをさらに備えることが好ましい。

【0015】なお、本発明によるデータ出力方法をコンピュータに実行させるプログラムとして、コンピュータ読取り可能な記録媒体に記録して提供してもよい。

【0016】

【発明の効果】本発明によれば、正規データを出力することが許可されなかった場合に、正規データに対応する疑似データを出力するようにしたため、不正アクセス者をあたかもアクセスに成功して正規データを入手したかのような錯覚に陥らせることができる。したがって、不正アクセス者にアクセス失敗を悟られることがなくなり、これにより正規データの不正な流出や、識別情報の解析等の不正行為を防止することができる。

【0017】また、取得した識別情報を所定形式の比較識別情報と比較し、識別情報が比較識別情報と異なる場合には、正規データおよび疑似データの出力を禁止する

ことにより、何回かアクセスに失敗した不正アクセス者が比較識別情報の形式と同一形式の識別情報を入力した際に疑似データが出力されることとなるため、不正アクセス者に対してあたかもアクセスに成功したかのように勘違いさせることが可能となる。

【0018】

【発明の実施の形態】以下図面を参照して本発明の実施形態について説明する。

【0019】図1は本発明の第1の実施形態によるデータ出力装置を適用したデータ出力システムの構成を示す概略ブロック図である。図1に示すように、このデータ出力システムは、本実施形態によるデータ出力装置1と、このデータ出力装置1にネットワーク2を介して接続された端末3とからなる。

【0020】データ出力装置1は、正規データTを蓄積した正規データベース4と、疑似データFを蓄積した疑似データベース5と、端末3から入力された識別情報Dを取得する識別情報取得手段6と、識別情報取得手段6により取得された識別情報Dに基づいて、識別情報Dに対応する正規データTの出力を許容するか否かを判断する判断手段7と、判断手段7により正規データTを出力することが許容された場合に、正規データTを端末3に出力する正規データ出力手段8と、判断手段7により正規データTを出力することが許容されなかった場合に、疑似データFを端末3に出力する疑似データ出力手段9とを備える。

【0021】判断手段7は、取得した識別情報Dが正規の識別情報であるか否かを判断し、識別情報Dが正規のものであると判断された場合に、この識別情報Dに対応する正規データTを正規データベース4から読み出して正規データ出力手段8によりネットワーク2を介して端末3に出力する。一方、取得した識別情報Dが正規のものでないと判断された場合には、この正規データTに対応する疑似データFを疑似データベース5から読み出して疑似データ出力手段9によりネットワーク2を介して端末3に出力する。

【0022】ここで、識別情報Dとしては、暗証番号、キーワード等端末3のアクセス者が端末3に設けられたキーボード等の入力手段から直接入力するものの他、端末3のIDや電話回線を介してアクセスがあった場合には、端末3の電話番号等、自動的に取得されるものを含む。

【0023】また、疑似データFとしては例えば正規データTが図2に示すような数値データである場合には、図3に示すように数値を並び替えたデータを用いる。このように、数値を並び替えた場合その合計値を並び替えた数値に対応させることにより、疑似データFをより正規データTらしく見せることができる。また、正規データTの数値の内容、桁数、データ形式を変更したものを疑似データFとしてもよい。なお、正規データTが画像

データである場合には、疑似データFを正規データTのように見えるが正規データTにより表される画像と類似した色調あるいは類似した構図の画像を表す画像データ等とすればよい。

【0024】次いで、第1の実施形態の動作について説明する。図4は第1の実施形態の動作を示すフローチャートである。まず、識別情報取得手段6において端末3から識別情報Dを取得する(ステップS1)。次に判断手段7において、取得した識別情報Dが正規のものであるか否かが判断される(ステップS2)。識別情報Dが正規のものである場合にはステップS2が肯定され、正規データベース4から識別情報Dに対応する正規データTを読み出し、正規データ出力手段8からネットワーク2を介して端末3に正規データTを出力する(ステップS4)。この場合、端末3の利用者は正規のアクセス者であることから、端末3においてはアクセス者が所望とする正規データTを得ることができる。

【0025】一方、識別情報Dが正規のものでない場合にはステップS2が否定され、疑似データベース5から疑似データFを読み出し、疑似データ出力手段9からネットワーク2を介して端末3に疑似データFを出力する(ステップS3)。この場合、端末3の利用者は不正アクセス者であることから、端末3においてはあたかもアクセスに成功したかのように疑似データFが得られる。

【0026】このように第1の実施形態によれば、不正アクセスがあった場合に、正規データTに対応する疑似データFを出力するようにしたため、不正アクセス者をあたかもアクセスに成功して正規データTを入手したかのような錯覚に陥らせることができる。したがって、不正アクセス者にアクセス失敗を悟られることがなくなり、これにより正規データTの不正な流出や、識別情報Dの解析等の不正行為を防止することができる。

【0027】なお、第1の実施形態においては、不正アクセスがあった場合に、疑似データベース5から疑似データFを読み出して端末3に出力しているが、図5に示す第2の実施形態のように、疑似データベース5に代えて、正規データTから疑似データFを作成する疑似データ作成手段10を備えるようにしてもよい。第2の実施形態においては、不正なアクセスがあった場合に、正規データベース4から正規データTを読み出し、この正規データTに基づいて疑似データ作成手段10において疑似データFを作成し、作成された疑似データFが疑似データ出力手段9よりネットワーク2を介して端末3に出力されることとなる。

【0028】次いで、本発明の第3の実施形態について説明する。図6は本発明の第3の実施形態によるデータ出力装置を適用したデータ出力システムの構成を示す概略ブロック図である。第3の実施形態は、判断手段7にて識別情報Dが予め登録された所定の形式であるか否かを判断し、所定の形式でありかつ正規の識別情報Dであ

る場合には正規データTを出力し、所定の形式でありかつ正規の識別情報Dでない場合には疑似データFを出力し、所定の形式でない場合には正規データおよび疑似データを出力することなくアクセスに失敗した旨を表すデータPを出力するようにした点が第1の実施形態と異なるものである。そして、第3の実施形態においては、このアクセスに失敗した旨を表すデータPを出力する出力禁止手段11を備えてなるものである。

【0029】第3の実施形態の判断手段7においては、図7(a)に示すような複数のダミーIDおよび図7(b)に示す真の登録IDが登録されている。本実施形態においては、判断手段7においてアクセスしている端末3のIDが判断され、その端末IDが正規のものである場合に、アクセス者が入力した識別情報Dが登録IDと比較される。ここで、本実施形態においては、複数の誕生日形式のダミーIDを登録しておき、登録されたダミーIDと同一形式の識別情報Dが入力された時にダミーIDと一致し、それ以外の形式の識別情報Dが入力された時にダミーIDと一致しないと判断するものである。

【0030】出力禁止手段11は、判断手段7による判断結果が登録ダミーIDと一致しないものである場合に、例えば「アクセス失敗」の表示を端末3で行うようなデータPをネットワーク2を介して端末3に出力するものである。

【0031】次いで、第3の実施形態の動作について説明する。図8は第3の実施形態の動作を示すフローチャートである。まず、識別情報取得手段6において端末3の識別情報Dおよびアクセスしている端末3の端末IDを取得する(ステップS11)。次に判断手段7において、取得した端末IDが正規の端末IDと一致するか否かが判断される(ステップS12)。取得した端末IDが正規の端末IDと一致する場合はステップS12が肯定され、さらに取得した識別情報Dが正規のものであるか否かが判断される(ステップS13)。識別情報Dが正規のものである場合には、正規データベース4から識別情報Dに対応する正規データTを読み出し、正規データ出力手段8からネットワーク2を介して端末3に正規データTを出力する(ステップS16)。この場合、端末3の利用者は正規のアクセス者であることから、端末3においてはアクセス者が所望とする正規データTを得ることができる。

【0032】一方、識別情報Dが正規のものでない場合にはステップS13が否定され、さらにステップS14において、識別情報Dが登録されたダミーIDと一致するか否かが判断される。識別情報DがダミーIDと一致する場合は疑似データベース5から疑似データFを読み出し、疑似データ出力手段9からネットワーク2を介して端末3に疑似データFを出力する(ステップS15)。この場合、端末3の利用者は不正アクセス者であ

ることから、端末3においてはあたかもアクセスに成功したかのような疑似データFが得られる。なお、ステップS12において端末IDが正規の端末IDでないと判断された場合にも、ステップS15において疑似データFが出力される。

【0033】さらに、識別情報DがダミーIDと一致しない場合には、正規データTおよび疑似データFの出力を禁止するとともに、出力禁止手段11からネットワーク2を介して端末3にデータPを出力する(ステップS17)。この場合、端末3にはアクセス失敗の旨の表示がなされることとなる。

【0034】このように第3の実施形態によれば、識別情報DをダミーIDと比較し、識別情報DがダミーIDと異なる場合には、正規データTおよび疑似データFの出力を禁止するとともに、アクセス失敗の旨を表すデータPを出力するようにしたため、何回かアクセスに失敗した不正アクセス者がダミーIDと同一形式の識別情報Dを入力した際には疑似データFが出力されることとなり、その結果、不正アクセス者に対してあたかもアクセスに成功したかのように勘違いさせることが可能となる。

【0035】なお、上記第3の実施形態においては、疑似データベース5から疑似データFを読み出して端末3に出力しているが、第2の実施形態のように、正規データTから疑似データFを作成するようにしてもよい。

【0036】また、上記第3の実施形態においては、ダミーIDを誕生日の形式としているが、これに限定されるものではなく、電話番号等任意の形式としてもよい。さらに、登録されたダミーIDと一致するか否かを判断しているが、例えば識別情報Dの桁数が予め登録した桁数と一致するか否かを判断するようにしてもよい。

【0037】さらに、上記第3の実施形態においては、ステップS12において端末IDが正規の端末IDでないと判断された場合に、ステップS15において疑似データFを出力しているが、ステップS17と同様に、正規データTおよび疑似データFの出力を禁止するとともにデータPを出力し、端末3においてアクセス失敗の旨を表示するようにしてもよい。

【0038】なお、上記各実施形態においては、端末3における正規のアクセス者が本当に正規データTを取得したか否かが分からなくなるおそれがある。したがって、正規データTを出力した後、利用者の登録住所への輸送、電話あるいはEメール等により、正規データTを出力した旨の立証をすることが好ましい。

【図面の簡単な説明】

【図1】本発明の第1の実施形態によるデータ出力装置を適用したデータ出力システムの構成を示す概略ブロック図

【図2】正規データの例を示す図

【図3】疑似データの例を示す図

【図4】第1の実施形態の動作を示すフローチャート

【図5】本発明の第2の実施形態によるデータ出力装置を適用したデータ出力システムの構成を示す概略ブロック図

【図6】本発明の第3の実施形態によるデータ出力装置を適用したデータ出力システムの構成を示す概略ブロック図

【図7】ダミーIDおよび真の登録IDを示す図

【図8】第3の実施形態の動作を示すフローチャート

【符号の説明】

1 データ出力装置

* 2 ネットワーク

3 端末

4 正規データベース

5 疑似データベース

6 識別情報取得手段

7 判断手段

8 正規データ出力手段

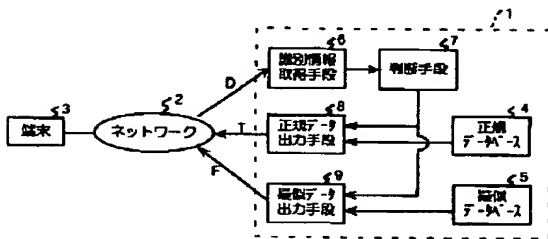
9 疑似データ出力手段

10 疑似データ作成手段

11 出力禁止手段

*

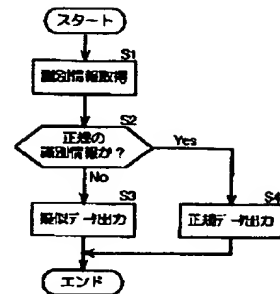
【図1】



【図2】

	A店	B店	C店	合計
1月度	123	456	789	1368
2月度	234	567	123	924
3月度	564	156	389	1109
合計	921	1179	1301	3401

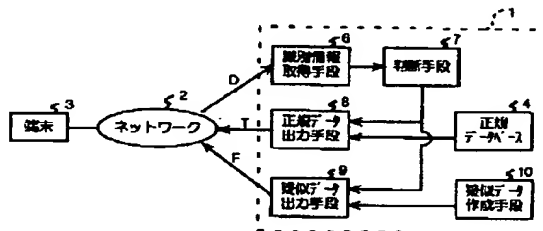
【図4】



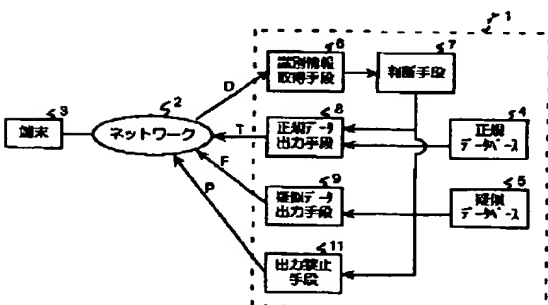
【図3】

	A店	B店	C店	合計
1月度	567	789	123	1479
2月度	123	456	156	735
3月度	789	389	564	1742
合計	1479	1634	843	3956

【図5】



【図6】



【図7】

(a)

登録ダミーID

端末ID AA12345

760521 870421

680118 640301

.....

端末ID AA12346

460221 771212

881207 811030

.....

(b)

真の登録ID

端末ID AA12345:590382, ...

端末ID AA12346:771111, ...

【図8】

